UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

IN RE: SAMSUNG DATA SECURITY BREACH LITIGATION

No. 1:23-md-03055
MDL 3055

This Document Relates To: ALL ACTIONS

OPINION

APPEARANCES:

James E. Cecchi
Caroline F. Bartlett
Jason H. Alperstein
CARELLA BYRNE CECCHI BRODY & AGNELLO, P.C.
5 Becker Farm Road
Roseland, NJ 07068

Interim Lead Counsel for Plaintiffs.

Kelly Iverson
LYNCH CARPENTER, LLP
1133 Penn Avenue
5th Floor
Pittsburgh, PA 15222

Roberta D. Liebenberg
Mary L. Russell
FINE, KAPLAN & BLACK
One S. Broad Street, 23rd Floor
Philadelphia, PA 19107

Nada Djordjevic
DICELLO LEVITT LLC
Ten North Dearborn Street, Sixth Floor
Chicago, IL 60602

Steven M. Nathan
HAUSFELD LLP
33 Whitehall Street, 14th Floor
New York, NY 10004

Sabita J. Soneji
TYCKO & ZAVAREEI LLP
1970 Broadway
Suite 1070
Oakland, California 94612

Ryan J. Clarkson
Yana Hart
CLARKSON LAW FIRM, P.C.
590 Madison Avenue
21st Floor
New York, NY 10022

Linda P. Nussbaum
NUSSBAUM LAW GROUP, P.C.
1133 Avenue of the Americas
31st Floor
New York, NY 10036-8718

Joseph J. DePalma
Catherine B. Derenze
LITE PALMA GREENBERG & AFANADOR, LLC
570 Broad Street, Suite 1201
Newark, NJ 07102

Christopher A. Seeger
Christopher L. Ayers
SEEGER WEISS LLP
55 Challenger Road, 6th Floor
Ridgefield Park, NJ 07660

Attorneys for Plaintiffs and Members of the Leadership Committee.

Maureen T. Coghlan
Carlos M. Bollar
ARCHER & GREINER, P.C.
1025 Laurel Oak Road
Voorhes, NJ 08043

Arthur E. Brown
Elie Salamon
ARNOLD & PORTER KAYE SCHOLLER LLP
250 West 55th Street
New York, NY 10019

Neil K. Gilman
Michael J. Mueller
Christopher J. Dufek
HUNTON ANDREWS KURTH LLP
2200 Pennsylvania Ave N.W.
Washington, D.C. 20009

Daniel E. Raymond
ARNOLD & PORTER KAYE SCHOLLER LLP
70 West Madison Street
Suite 4200
Chicago, IL 60602

On behalf of Defendant.

O'HEARN, District Judge.

This matter comes before the Court on a Motion to Dismiss Plaintiffs' Fourth Amended Consolidated Complaint for Lack of Jurisdiction pursuant to Federal Rule of Civil Procedure 12(b)(1), or alternatively for Failure to State a Claim pursuant to Federal Rule of Civil Procedure 12(b)(6), and a Motion to Strike Class Allegations by Defendant Samsung Electronics America, Inc. ("Defendant" or "Samsung"). (ECF Nos. 161, 163). For the reasons that follow, Defendant's Motion to Dismiss for Lack of Jurisdiction is **GRANTED** and the Motion to Strike is therefore **DENIED** as moot.

I. BACKGROUND

This putative class action arises out of an unauthorized third-party's exfiltration of Defendant's [redacted]. (Fourth Am. Compl., ECF No. 147, ¶ 1). Specifically, in July 2022, Defendant was the victim of a criminal attack in which an unauthorized third party acquired information from Defendant's [redacted]. (*Id.* at ¶ 12). On August 4, 2022, Samsung discovered that the personal information of some of its customers was exfiltrated. (*Id.* at ¶ 47). On September 2, 2022, Defendant disclosed the data breach in a notice posted on its website and emailed to its customers ("the Notice"), which Plaintiffs allege was inadequate as to (1) the origin of the breach, (2) how it was uncovered, (3) the scope of the systems affected, (4) the reason for the delay in notifying affected customers, and (5) the extent of customer data accessed, among other information. (*Id.* at ¶¶ 12–14, 46–61). The Notice stated that the breach may have affected customers' Personal Identifying Information ("PII") such as "name, contact, demographic[s], date of birth, and product registration number." (*Id.* at ¶¶ 13, 48). However, Plaintiffs allege that the PII stolen in the data breach included "one or more of the following categories of information:"

- Full names;
- Dates of birth;
- Samsung account data and account credentials, including . . . Samsung account unique user ID;
- Personal identifiers and contact information such as email addresses, postal addresses, telephone numbers, IP addresses, country code, and region;
- Demographic data, such as age and age range, gender, marital status . . ., number (if any) of children, occupation/vocation, income range . . ., race and ethnicity[;]

- Product registration information, such as IMEI (International Mobile Equipment Identity)[;] and

- Financial information, such as method of payment.

(*Id*. at ¶¶ 3, 14). Plaintiffs allege this information is very valuable. (*Id*. at ¶ 64).

Indeed, when purchasing a Samsung product, creating an account, or registering for a service, customers provide Samsung with various PII:

> name; email address; postal address; phone number; payment card information (including name, card number, expiration date, and security code); date of birth; demographic information, *e.g.*, gender and age range; information stored in or associated with the customer's Samsung account, including the customer's Samsung Account profile, ID, username, and password; username and password for participating third-party devices, apps, features, or services; information a customer stores on a Samsung device, such as photos, contacts, text logs, touch interactions, settings, and calendar information; recordings of a customer's voice when they use voice commands to control a service or contact Samsung's Customer Service team; transcripts of chat sessions, text messages, emails, and other communications when the customer communicates with Samsung using these methods; information about products and services that customers purchase, obtain, or consider; and location data, including (1) the precise geolocation of a customer's device if the customer consents to the collection of this data; and (2) information about nearby Wi-Fi access points and cell towers that may be transmitted to Samsung when the customer uses certain [s]ervices.

(*Id.* at ¶ 25). In addition to this information, Samsung also collects "browser cookies, pixels, web server logs, web beacons, and other technologies[.]" (*Id*. at ¶ 26). Samsung promises customers it will keep their data secure in various privacy policies and notices. (*Id*. at ¶¶ 34–35).

Despite these assurances, Plaintiffs allege Defendant's lax security practices have resulted in multiple disclosures of customers' PII, including this breach. (*Id.* at ¶ 38). Plaintiffs allege the possible involvement by a cybercrime hacking group known as [redacted]. (*Id*. at ¶ 17).

As a result of the July 2022 data breach, Plaintiffs allege they have been injured in a variety of ways, including:

> (1) loss of value of PII, (2) monetary loss through out-of-pocket expenses associated with preventing and remediating identity theft, (3) opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, (4) increased risk that unauthorized persons will access and abuse Plaintiffs' PII, (5) continued risk that the PII remains in Defendant's possession (6) invasion of privacy, (7) increased risk to personal safety, (8) loss of privacy rights, and (9) emotional distress.

(*Id*. at ¶ 7). Plaintiffs also allege that with the IMEI numbers, "hackers can track a phone's location, . . . engage in fraudulent activities, . . . or access bank accounts and financial information." (*Id*. at ¶ 14).

Plaintiffs bring this class action alleging the following class-wide claims: (1) negligence (Count One); (2) negligence *per se* (Count Two); (3) breach of express contract (Count Three); (4) breach of implied contract (Count Four); (5) unjust enrichment (Count Five); and (6) declaratory judgment (Count Six). (*Id.* at ¶¶ 301–48). Plaintiffs also bring forty-nine different claims on behalf of the subclasses. (*Id.* at ¶¶ 349–863).

II. PROCEDURAL HISTORY

This action encompasses sixteen separate cases pending in eleven different courts around the country. (ECF Nos. 1, 3). On February 1 and 10, 2023, all the cases were transferred to this Court and consolidated for pretrial purposes by order of the United States Judicial Panel on Multidistrict Litigation. (*Id.*). During the initial conference on April 6, 2023, Plaintiffs sought to begin full discovery, which Defendant opposed. (ECF No. 38 at 8:15–16:3). The Court ordered the parties to meet and confer as to a scheduling order and to begin discovery by exchanging fact sheets ("Fact Sheets"). (*Id*.; ECF No. 40). On May 22, 2023, Plaintiffs filed their first Amended

Consolidated Complaint against Defendant, which was later corrected on May 24, 2023. (ECF Nos. 48–49). On July 10, 2023, the Court appointed the Honorable Freda Wolfson, retired United States District Chief Judge, to serve as Special Master. (ECF No. 69). On July 14, 2023, Plaintiffs filed a second Amended Consolidated Complaint. (ECF No. 72).

On August 11, 2023, Defendant filed a Motion to Dismiss the Second Amended Consolidated Complaint and a Motion to Strike the Class Allegations. (ECF Nos. 84–85). Plaintiffs filed opposition to both Motions on September 22, 2023, to which Defendant replied on October 20, 2023. (ECF Nos. 93–94, 100–01). The Court held a status conference on February 1, 2024, to identify for counsel the key issues presented in the Motions for the upcoming scheduled oral argument on February 7, 2023. (ECF No. 117). During the conference, Plaintiffs' interim lead counsel informed the Court that the case had developed since the Motions' initial briefing as a result of having received Defendant's responses to the Fact Sheets. (*Id*. at 11:6–14). Plaintiffs' counsel proposed amending the Complaint. (*Id*. at 13:12). Following the status conference, the Court ordered that Plaintiffs submit an Amended Complaint within ten days and set a briefing schedule for supplemental briefing. (ECF No. 118).

Plaintiffs filed a Third Amended Consolidated Complaint on February 13, 2024. (ECF No. 120). During a status conference on March 7, 2024, defense counsel informed the Court that the Third Amended Consolidated Complaint had "fundamentally changed the approach to this case" and with the understanding that after "information is brought forward, complaints can evolve," Defendant requested the opportunity to file new briefing because the motions Defendant sought to file differed from those then pending. (ECF No. 129 at 5:2–20). During this conference, Plaintiffs' counsel emphasized that the information they learned through the Fact Sheets was more "granular

detail about the massive nature of this data breach," and agreed with Defendant's proposal to file new briefing in light of the new factual allegations, which the Court permitted. (*Id*. at 6:5–22).

Plaintiffs filed a Fourth Amended Consolidated Complaint on April 11, 2024. (ECF No. 147). The Fourth Amended Consolidated Complaint encompasses the allegations of forty-one Plaintiffs from twenty-nine states. (*Id*.). On May 22, 2024, Defendant moved to dismiss each cause of action for lack of standing or alternatively, because they are unsupported by the factual allegations in the Complaint. (ECF No. 161). That same day, Defendant also moved to strike class allegations. (ECF No. 163). On July 2, 2024, Plaintiffs filed briefs in opposition to Defendant's Motion to Dismiss and Strike Class Allegations. (ECF Nos. 173–74). Defendant filed replies on August 2, 2024. (ECF Nos. 185–86).

III. LEGAL STANDARDS

A. Standing

Pursuant to Article III of the Constitution, this Court may only exercise jurisdiction to resolve "Cases" and "Controversies." U.S. CONST. art. III, § 2, cl. 1. "Thus, federal courts can entertain actions only if they present live disputes, ones in which both sides have a personal stake." *Hartnett v. Pa. State Educ. Ass'n*, 963 F.3d 301, 305 (3d Cir. 2020). As the party invoking federal jurisdiction at the start of litigation, the plaintiff bears the burden of establishing Article III standing. *Id.* Additionally, in the class action context, "[e]ach named plaintiff . . . must personally demonstrate standing independently of any claims brought on behalf of a putative class." *Bycko v. State Farm Mut. Auto. Ins. Co.*, No. 23-1316, 2023 WL 7411752, at *5 (D.N.J. Nov. 9, 2023) (citing *In re Am. Med. Collection Agency, Inc. Customer Data Sec. Breach Litig.*, No. 19-2904, 2021 WL 5937742, at *6 (D.N.J. Dec. 16, 2021)).

To establish standing, a plaintiff must show (1) "that he [or she] suffered an injury in fact that is concrete, particularized, and actual or imminent;" (2) "that the injury was likely caused by the defendant;" and (3) "that the injury would likely be redressed by judicial relief." *TransUnion LLC v. Ramirez*, 594 U.S. 413, 422–23 (2021) (citing *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560–61 (1992)). "If 'the plaintiff does not claim to have suffered an injury that the defendant caused and the court can remedy, there is no case or controversy for the federal court to resolve.'" *TransUnion*, 594 U.S. at 423 (quoting *Casillas v. Madison Ave. Assocs., Inc.*, 926 F.3d 329, 333 (7th Cir. 2019)). The injury must be "'concrete'—that is, 'real, and not abstract.'" *Id.* at 424 (quoting *Spokeo, Inc. v. Robins*, 578 U.S. 330, 340 (2016)).

When a plaintiff fails to establish Article III standing, the court lacks subject matter jurisdiction, *Finkelman v. Nat'l Football League*, 810 F.3d 187, 195 (3d Cir. 2016), and dismissal is required, *Goodmann v. People's Bank*, 209 F. App'x 111, 113 (3d Cir. 2006); FED. R. CIV. P. 12(b)(1). Where the named plaintiffs fail to establish Article III standing, the putative class action must be dismissed for lack of subject matter jurisdiction. *Finkelman*, 810 F.3d at 195. Additionally, courts may "dismiss a suit *sua sponte* for lack of subject matter jurisdiction at any stage in the proceeding." *Zambelli Fireworks Mfg. Co., Inc. v. Wood*, 592 F.3d 412, 420 (3d Cir. 2010); FED. R. CIV. P. 12 (h)(3).

B. Federal Rule of Civil Procedure 12(b)(6)

To state a claim, a complaint needs only to provide a "short and plain statement of the claim showing that the pleader is entitled to relief." FED. R. CIV. P. 8(a)(2). Although "short and plain," this statement must "give the defendant fair notice of what the claim is and the grounds upon which it rests." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 545 (2007) (quotations, alterations,

and citation omitted). "[A] plaintiff's obligation to provide the 'grounds' of his 'entitle[ment] to relief' requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Id.* (citations omitted). Rather, a complaint must contain sufficient factual allegations "to state a claim to relief that is plausible on its face." *Id.* at 547.

When considering a motion to dismiss for failure to state a claim under Federal Rule of Civil Procedure 12(b)(6), a court must accept the complaint's well-pleaded allegations as true and view them in the light most favorable to the plaintiff. *Evancho v. Fisher*, 423 F.3d 347, 350 (3d Cir. 2005). Through this lens, the court then conducts a three-step analysis. *Malleus v. George*, 641 F.3d 560, 563 (3d Cir. 2011). "First, the court must 'tak[e] note of the elements a plaintiff must plead to state a claim.'" *Id.* (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 675 (2009)). Next, the court should identify and disregard those allegations that, because they are no more than conclusions, are not entitled to the assumption of truth. *Id.* Finally, the court must determine whether "the facts alleged in the complaint are sufficient to show that the plaintiff has a 'plausible claim for relief.'" *Fowler v. UPMC Shadyside*, 578 F.3d 203, 211 (3d Cir. 2009) (quoting *Iqbal*, 556 U.S. at 679). A facially plausible claim "allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* at 210 (quoting *Iqbal*, 556 U.S. at 678).

On a Federal Rule of Civil Procedure 12(b)(6) motion, the "defendant bears the burden of showing that no claim has been presented." *Hedges v. United States*, 404 F.3d 744, 750 (3d Cir. 2005). The court may only consider the facts alleged in the pleadings, any attached exhibits, and any matters of judicial notice. *S. Cross Overseas Agencies, Inc. v. Kwong Shipping Grp. Ltd.*, 181 F.3d 410, 426 (3d Cir. 1999).

IV. DISCUSSION

Defendant has moved to dismiss the Fourth Amended Consolidated Complaint, arguing that Plaintiffs lack Article III standing because (1) Plaintiffs' theories of harm do not constitute an injury-in-fact; and (2) Plaintiffs' allegations of attempted and actual identity theft or fraud cannot be traced to the exfiltrated information. (Def. Br., ECF No. 162 at 14). In addition to these threshold issues, Defendant argues that Plaintiffs have failed to plead cognizable damages and that all of Plaintiffs' claims are barred by the liability clause in Samsung's Account Terms & Conditions ("T&C"). (*Id*. at 35, 51). Finally, Defendant also contends that Plaintiffs' common law and statutory causes of action all fail to state a claim. (*Id*. at 76–109). In response, Plaintiffs maintain that they have Article III standing because they sufficiently plead injury-in-fact, imminent risk of future identity theft, and injuries that are traceable to Defendant's conduct. (Pla. Br., ECF No. 174 at 10–29). Plaintiffs further argue that the allegations sufficient to confer standing also establish damages at this stage. (*Id*. at 36). Plaintiffs deny that their claims are barred by the liability clause in the T&C and argue that they have adequately pled the common law and statutory claims. (*Id*. at 51–120).

The Court will grant Defendant's Motion to Dismiss for lack of Article III standing.

A. Standing

As a threshold issue, the Court must first determine whether Plaintiffs have established Article III standing such that the Court has subject matter jurisdiction over this action. Here, after four attempts to do so, Plaintiffs have failed to meet their burden.

To establish the injury-in-fact prong, the injury must be "actual or imminent, not 'conjectural' or 'hypothetical.'" *Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 152 (3d Cir. 2022)

(citing *Lujan*, 504 U.S. at 560). To show "actual or imminent" injury, the Third Circuit in *Clemens*, a data breach case, explained the "'actual or imminent' disjunctive is critical: it indicates that a plaintiff need not wait until he or she has *actually* sustained the feared harm . . . to seek judicial redress." *Id*. (emphasis in original). "[A]llegations of future harm 'suffice if the threatened injury is 'certainly impending' or there is a 'substantial risk' that the harm will occur.'" *Id*. (citing *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014)). But when a "future injury is also hypothetical, there can be no imminence and therefore no injury-in-fact." *Id*. at 153.

In *Reilly v. Ceridian Corporation*, the Court considered "whether an alleged risk of future identity theft or fraud stemming from a data breach in which an unknown hacker potentially accessed sensitive personal and financial information from a company's network was sufficiently imminent for purposes of standing." *Clemens*, 48 F.4th at 153 (citing *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011)). "Because the plaintiffs in *Reilly* alleged a future, hypothetical risk of identity theft or fraud, [the Third Circuit] concluded that they had not suffered an injury-in-fact." *Id*. (citing *Reilly*, 664 F.3d at 42). There, the future harm was "dependent on entirely speculative, future actions of an unknown third-party." *Reilly*, 664 F.3d at 42. The Court noted that it could not "describe how [the plaintiffs] will be injured in th[e] case without beginning [its] explanation with the word 'if': *if* the hacker read, copied, and understood the hacked information, and *if* the hacker attempts to use the information, and *if* he does so successfully, only then will [the plaintiffs] have suffered an injury." *Id*. at 43 (emphasis in original). The *Reilly* Court in concluding the plaintiffs did not have standing also considered that there was no evidence that the exfiltration was intentional or malicious, that the plaintiffs had not alleged misuse, and that no identifiable taking had occurred. *Id*. at 44.

Thereafter in *Clemens*, the Third Circuit clarified that it did not create a "bright line rule" in *Reilly* precluding standing based on identity theft or fraud. *Clemens*, 48 F.4th at 153. "Instead, *Reilly* requires consideration of whether an injury is present versus future, and imminent versus hypothetical." *Id*. In determining whether an injury is imminent, the Third Court listed non-exhaustive factors courts should consider—none being dispositive: (1) whether the data breach was intentional; (2) whether the data was misused; and (3) whether the nature of the information accessed through the data breach could subject a plaintiff to a risk of identity theft (*i.e.*, disclosure of social security numbers, birth dates, and names—though, disclosure of financial information alone, without corresponding personal information, is insufficient). *Id*. at 154. In determining whether the injury is concrete—that is, "real, and not abstract"—"where the asserted theory of injury is a substantial risk of identity theft or fraud, a plaintiff suing for damages can satisfy concreteness as long as he alleges that the exposure to that substantial risk caused additional, currently felt concrete harms." *Id*. at 155–56.

Applying these principles in *Clemens*, the Court concluded that the plaintiff alleged a future injury that was sufficiently imminent because (1) the breach was conducted by a known hacking group, which intentionally stole the information, held it for ransom, and published it on the Dark Web, making it accessible to criminals worldwide; and (2) the nature of the information—a combination of personal and financial information—was the type of data that could be used to perpetrate identity theft or fraud. *Id*. at 159. Moreover, because intangible harms like the publication of personal information can qualify as concrete, the risk of identity theft or fraud in *Clemens* constituted an injury-in-fact. *Id*.

Since *Clemens*, courts in this Circuit have analyzed standing in data breach cases using the three-factor test outlined therein. *See, e.g., Alonzo v. Refresco Beverages US, Inc.*, No. 23-22695, 2024 WL 4349592, at *5 (D.N.J. Sept. 30, 2024).

1. Injury-in-Fact: Imminence

a. Whether the breach was intentional.

Beginning with the first factor, the Court evaluates this factor keeping in mind that "all cyber-attacks involve some degree of intentional conduct just by the very nature of the attack." *Alonzo*, 2024 WL 4349592, at *5 (quoting *McGowan v. CORE Cashless, LLC*, No. 23-00524, 2023 WL 8600561, at *9 (W.D. Pa. Oct. 17, 2023), *R. & R. adopted*, No. 23-00524, 2024 WL 488318 (W.D. Pa. Feb. 8, 2024)). Additionally, the Third Circuit deemed this factor satisfied in *Clemens* based on the plaintiff's allegation that "CLOP," "a sophisticated ransomware group," accessed the plaintiff's data, held it for ransom, and then published it on the Dark Web. *Clemens*, 48 F.4th at 157.

Here, Plaintiffs allege that [redacted] (Am. Compl., ECF No. 147, ¶ 17). Unlike *Reilly* and *Alonzo* in which the plaintiffs merely alleged that the hackers were an "unknown third party," Plaintiffs here specify a known criminal hacking group that may have been involved in the attack. *See* (*id.*). Even if [redacted] is ultimately found not to have been involved, Plaintiffs' allegation that [redacted] is sufficiently suggestive that the attack was intentional. *Compare Roma v. Prospect Med. Holdings,*

Inc., No. 23-3216, 2024 WL 3678984, at *5 (E.D. Pa. Aug. 6, 2024) (finding intentionality when ransomware gang takes responsibility for the data breach) *with In re Retreat Behav. Health LLC*, No. 23-00026, 2024 WL 1016368, at *3 (E.D. Pa. Mar. 7, 2024) (finding plaintiff who alleged that an "unknown hacker who potentially gained access to sensitive information" did not have standing) *and In re Am. Fin. Res., Inc. Data Breach Litig.*, No. 22-01757, 2023 WL 3963804, at *5 (D.N.J. Mar. 29, 2023) (concluding a plaintiff alleging a "criminal" hack by unknown individuals that could not "meaningfully allege that the information accessed in the breach was mass-published onto the dark web, or otherwise disseminated" lacked standing). Though, unlike *Clemens*, Plaintiffs do not allege that the data was held for ransom or universally published on the Dark Web, the allegation that it was an attack by a known cybergang is sufficiently suggestive of intentionality at this stage. This factor, thus, weighs in favor of a finding of imminent harm.

b. Whether the data was misused.

Although whether the data was misused, is not *required* to allege an injury-in-fact, *Clemens*, 48 F.4th at 154, it is a consideration. *See McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295, 301–02 (2d Cir. 2021) (holding that misuse cuts in favor of standing); *In re Equifax Inc. Customer Data Sec. Breach Litig.*, 999 F.3d 1247, 1262 (11th Cir. 2021) ("The actual identity theft already suffered by some Plaintiffs further demonstrates the risk of identity theft all Plaintiffs face—though actual identity theft is by no means required when there is a sufficient risk of identity theft."); *Remijas v. Neiman Marcus Grp.*, 794 F.3d 688, 692–94 (7th Cir. 2015) (finding standing where plaintiff alleged that personal data had "already been stolen" and that 9,200 people had "incurred fraudulent charges"); *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1142–43 (9th Cir. 2010) (finding standing where a laptop with personal unencrypted data

was stolen and plaintiff alleged that someone "attempted to open a bank account in his name"); *In re 21st Century Oncology Customer Data Sec. Breach Litig.*, 380 F. Supp. 3d 1243, 1254 (M.D. Fla. 2019) (noting that an increased risk of identity theft is "more likely to constitute an injury in fact where there is evidence that a third-party has accessed the sensitive information and/or already used the compromised data fraudulently"); *In re Am. Fin. Res., Inc. Data Breach Litig.*, 2023 WL 3963804, at *5 ("Like in *Reilly*, Plaintiffs cannot meaningfully allege that the information accessed in the breach was mass-published onto the Dark Web, or otherwise disseminated."); *Boje v. Mercyhurst Univ.*, No. 23-46, 2024 WL 964892, at *4 (W.D. Pa. Mar. 6, 2024) ("Unlike in *Clemens*, there is no allegation that the information compromised by the Data Breach in the present case was ever published on the Dark Web or otherwise distributed or made available to 'nefarious' third parties.").

Here, there are no allegations that [redacted] or any other group published the data on the Dark Web, unlike cases in which courts have found intentionality. *See Clemens*, 48 F.4th at 150, 157. Some Plaintiffs merely allege that they have been notified that their data is on the Dark Web and generally state that [redacted] (Am. Compl., ECF No. 147, ¶ 87) (emphasis added).

In fact, out of forty-one Plaintiffs, only four allege that they have been notified that their "personal information" is on the Dark Web. Even more problematic is that all four of the Plaintiffs that make this allegation do so without specifying that it was the *specific information* that was obtained in this data breach versus information obtained elsewhere, *i.e.* social security numbers and credit card information, that was not a part of this breach. Moreover, as discussed below, the

information these four Plaintiffs allege they provided Samsung—certain personal identifiers and contact information, device data, including IMEI number(s), and IP address—is not the type of information that historically has been recognized as sufficiently sensitive and subjecting them to an increased risk of identity fraud.

But even if this factor weighs in favor of imminence for these *four* Plaintiffs, "these allegations [do] not suffice to show that the same will happen to Plaintiffs who have not alleged facts indicating that their PII was accessed and disseminated." *In re Am. Fin. Res., Inc. Data Breach Litig.*, 2023 WL 3963804, at *5; *see also Lujan*, 504 U.S. at 563 (quoting *Sierra Club v. Morton*, 405 U.S. 727, 734–35 (1972) ("[T]he 'injury in fact' test requires more than an injury to a cognizable interest. It requires that the party seeking review be himself among the injured.")); *In re Am. Med. Collection Agency, Inc.*, 2021 WL 5937742, at *10 ("[T]hat others have suffered some concrete injury following the Data Breach is insufficient to establish the particularized reasonableness of these plaintiffs' fears of future harm."); *McGowan*, 2024 WL 488318, at *3 (noting no misuse where "[p]laintiff has failed to allege sufficient facts to plausibly show that *her* payment card information was misused by the unknown hackers"). And as discussed below, *see infra* Section IV.B, though these four Plaintiffs might be able to show misuse, it is not traceable to Defendant.

For the remaining thirty-seven Plaintiffs, none allege that some actor has actually misused the specific PII obtained in the data breach or published their information on the Dark Web. And as Defendant aptly notes, it has been two years since the security breach and yet, there are no allegations of actual misuse. *See Kylie S. v. Pearson PLC*, 475 F. Supp. 3d 841, 847 (N.D. Ill. 2020) ("Plaintiffs' inability to identify any consequences of the data breach reinforces that

conclusion. More than a year after the breach, Plaintiffs cannot point to a single instance of identity theft affecting any of the 900,000 members of the putative class."). Instead, Plaintiffs merely allege that [redacted] has "all the information it needs . . . to sell the data on the Dark Web," but not that it, or any other third party, has sold the information. (Am. Compl., ECF No. 147, ¶¶ 19, 87).

As for Plaintiffs' allegations of unauthorized charges, credit inquiries, fraudulent attempts to create accounts, and various hacked accounts, there is no allegation that any of these Plaintiffs even provided the type of information needed to commit these types of identity theft, *i.e.*, financial account information or username or passwords for the accounts to Samsung. Indeed, in *Kim v. McDonald's USA, LLC*, the Court, in dismissing the plaintiffs' complaint for lack of standing, explained that unless the plaintiffs used their cell phone numbers or street addresses—the information obtained in the hack—as the passwords for their email or other accounts which they allege were hacked, "potential hackers would still need to resort to other methods to gain access to Plaintiffs' accounts. The claimed future harm would require a 'highly attenuated chain of possibilities' to materialize and finding such harm would 'require guesswork as to how independent decisionmakers will exercise their judgment.'" No. 21-05287, 2022 WL 4482826, at *5 (N.D. Ill. Sept. 27, 2022) (quoting *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 407 (2013)). Similarly, here, Plaintiffs' speculative allegation of future potential misuse requires a "highly attenuated chain of possibilities" which "requires guesswork" given the innocuous nature of the information obtained in the breach.

Additionally, increased phishing, also alleged by Plaintiffs, has been rejected by courts as insufficient to allege future harm. In *Kim*, the Court reasoned that even assuming that phishing attempts can be traced to the data breach, allegations of phishing attempts, alone, without any

materialized theft is insufficient. *See* 2022 WL 4482826, at *5; *see also McCombs v. Delta Grp. Elecs., Inc.*, 676 F. Supp. 3d 1064, 1074 (D.N.M. 2023) ("Spam calls . . . have become very common in this digitized world, and a number of courts have declined to confer standing when considering an increase in spam communications."); *I.C. v. Zynga, Inc.*, 600 F. Supp. 3d 1034, 1052 (N.D. Cal. 2022) (explaining allegations of "various forms of spam . . . fall short of actual identity theft," particularly where there are no allegations that these attempts were successful); *Williams v. Bienville Orthopedic Specialists, LLC*, No. 23-232, 2024 WL 3387169, at *5 (S.D. Miss. June 18, 2024) (collecting cases) (determining the plaintiff's allegation of an increase in spam calls is insufficient to establish an injury in fact); *Cooper v. Bonobos, Inc.*, No. 21-854, 2022 WL 170622, at *5 (S.D.N.Y. Jan. 19, 2022) (noting that "[c]ourts have generally rejected the theory that unsolicited calls or emails constitute an injury in fact").

Thus, to the extent the allegations of Plaintiffs Kelechian, Peavy, Allen, and Baker, that their information is on the dark web suffices to show misuse, it certainly does not for the remaining Plaintiffs. *See Reilly*, 664 F.3th at 45 ("In data breach cases where no misuse is alleged, however, there has been no injury—indeed, no change in the status quo.").

c. The nature of the information accessed.

However, and most critical here, the third factor is decisively fatal for all Plaintiffs. In fact, and as Defendant notes, Plaintiffs' allegations in this regard even fall short of those in *Reilly*, where the Third Circuit concluded that plaintiffs did not have standing. Put simply, the information the parties now agree was accessed in the data breach—names, addresses, other contact and demographic information, and device information—is not the type of PII that subjects an

individual to a heightened risk of identity theft or fraud in any way despite Plaintiffs' repeated attempts to suggest otherwise.

Plaintiffs allege that their names, addresses, other contact and demographic information, and device information were obtained in the breach. (Am. Compl., ECF No. 147, ¶ 3). Yet, courts routinely have dismissed claims for lack of jurisdiction when the information accessed is similar, or in some cases, even more sensitive to that which Plaintiffs allege here because the risk of future harm is far too attenuated or speculative. *Compare McGowan*, 2023 WL 8600561, at *1, *11 (concluding that disclosure of "names, addresses, email addresses, phone numbers, and payment card information" was "not likely to subject Plaintiff to a substantial risk of identity theft or fraud"); *Kim*, 2022 WL 4482826, *4 ("With respect to potential future harms, Plaintiffs fail to plausibly allege that the harm they fear—identity theft and being victimized by a phishing scam—is impending. The type of data stolen in the data breach consisted of non-sensitive email addresses, phone numbers, and delivery addresses."); *In re Uber Techs., Inc., Data Sec. Breach Litig.*, No. 18-2970, 2019 WL 6522843, at *4 (C.D. Cal. Aug. 19, 2019) ("Plaintiff fails to explain how gaining access to one's basic contact information and driver's license number creates a credible threat of fraud or identity theft."); *Antman v. Uber Techs., Inc.*, No. 15-01175, 2015 WL 6123054, at *11 (N.D. Cal. Oct. 19, 2015) ("Without a hack of information such as social security numbers, account numbers, or credit card numbers, there is no obvious, credible risk of identity theft that risks real, immediate injury.") *with Clemens*, 48 F.4th at 154 ("[D]isclosure of social security numbers, birth dates, and names is more likely to create a risk of identity theft or fraud"); *In re Horizon Healthcare Servs. Inc. Data Breach Litig.*, 846 F.3d 625, 630, 639 n.19 (3d Cir. 2017) (describing stolen information such as "name and demographic information . . . and in some

instances, a Social Security number and/or limited clinical information" as "highly personal and could be used to steal one's identity" as suggestions of what creates a material risk of harm); *In re Fortra File Transfer Software Data Sec. Breach Litig.*, No. 23-60830, 2024 WL 4547212, at *35 n. 4 (S.D. Fla. Sept. 18, 2024) (citation and internal quotation marks omitted) ("Static information like Social Security numbers, birth dates, driver's license numbers, and health insurance information is particularly valuable to thieves and the theft of such data will weigh in favor of a finding of injury in fact.") ; *Roma*, 2024 WL 3678984, at *1, *5 (concluding information sufficient to create risk of identity theft when the data breach had exposed customers' "full names, Social Security numbers, addresses, dates of birth, driver's license numbers, . . . financial information[,] diagnosis information, lab results, prescription information, treatment information, health insurance information, claims information, and medical record numbers."); *Adkins v. Everest Global Servs., Inc.*, No. 23-004, 2024 WL 3887127, at *5 (D.N.J. Aug. 21, 2024) (concluding that name and social security number is the kind of information sufficient to plausibly create a heightened risk of identity theft).

In fact, given the current frequency of data breaches, there is a surplus of caselaw involving non-sensitive information, such as here, that have been repeatedly dismissed as a matter of course. *See Kim*, 2022 WL 4482826, at *5 (collecting cases); *see e.g.*, *Kylie S.*, 475 F. Supp. 3d at 848 ("In short, Plaintiffs' theory fails because the disclosed data [names, emails, and birthdays] is not sensitive enough to materially increase the risk of identity theft."); *De Medicis v. Ally Bank*, No. 24-6799, 2022 WL 3043669, at *10 (S.D.N.Y. Aug. 2, 2022) (citation and internal quotation marks omitted) ("Instead, as alleged, Plaintiff's username and password appears to be less sensitive information that can be rendered useless to cybercriminals and does not pose the same risk of

future identity theft or fraud to plaintiffs if exposed."); *Fus v. CafePress, Inc.*, No. 19-06601, 2020 WL 7027653, at *3 (N.D. Ill. Nov. 30, 2020) ("[M]ost of Fus's information possessed by CafePress at the time of the hack was publicly available information, such as his billing and shipping address and personal email address. However, the disclosure of such information does not expose Fus to a significant risk of identity theft or fraud."); *In re Vtech Data Breach Litig.*, No. 150-10889, 2017 WL 2880102, at *4 (N.D. Ill. July 5, 2017) ("Plaintiffs have not shown an increased risk of identity theft due to a data breach because they do not allege how the stolen data would aid identity thieves in their efforts."); *Cooper*, 2022 WL 170622, at *5 ("Put simply, given the nature and age of the data, the likelihood that its exposure would result in harm to Cooper is too remote to support standing.").

As for Plaintiffs' allegation that their IMEI numbers were obtained, Plaintiffs allege that this information when (1) *paired* with other personal information and (2) with the "assistance of an insider at a telecommunication company" could be used to "clone" a phone. (Am. Compl., ECF No. 147, ¶¶ 14, 95). But the *Clemens* Court noted that even general financial information *alone* is insufficient to give rise to an imminent threat of identity theft or fraud. 48 F.4th at 154 ("By contrast, the disclosure of financial information alone, without corresponding personal information, is insufficient" because "financial information alone generally cannot be used to commit identity theft or fraud"). Similarly, an IMEI number, alone, is insufficient.

And Plaintiffs' argument that the information may be used for social engineering—like SIM swapping and port scanning—has been rejected by other courts. For example, the Court in *Kylie S. v. Pearson PLC*, in determining whether there was an increased risk of identity theft such to establish standing, also considered the sensitivity of the data in question. 475 F. Supp. 3d at 846.

There, hackers accessed a database containing first and last names, dates of birth, email addresses, and for some of the plaintiffs, their unique student identification numbers. *Id*. at 844. In concluding that the hack did not increase the plaintiffs' risk of identity theft, the Court explained "[w]hat matters most is that the data disclosed here is far less likely to facilitate identity theft than the credit and debit card numbers at issue in [other cases]." *Id*. at 846. Though the Court acknowledged, as had been raised in the complaint, that "social engineering"—in which a hacker obtains benign information and then contacts IT help desks at companies to obtain more sensitive information—is a tactic used by hackers, "any theory that the data would facilitate social engineering depends on a 'highly attenuated chain of possibilities' that 'does not satisfy [Article III] standing.'" *Id*. at 847 (quoting *Clapper*, 568 U.S. at 410). Social engineering often involves a "long sequence of uncertain contingencies involving multiple independent actors." *Id*. (quoting *Attias v. Carefirst, Inc.*, 865 F.3d 620, 629 (D.C. Cir. 2017)). "In other words, social engineering only poses a threat if exceptionally determined hackers encounter especially credulous IT personnel. While that combination is theoretically possible, nothing in the complaint establishes that it exposes Plaintiffs to a substantial risk." *Id*. Like *Kylie S.*, here, Plaintiffs' social engineering theory, which too depends on a "highly attenuated chain of possibilities," does not establish Article III standing.

Other courts, like the Northern District of Illinois, have similarly found, noting it is "unclear how the disclosure of plaintiffs' names, addresses, birthdates, and VTech account information would increase the risk of fraudulent transactions on plaintiffs' credit cards or fraudulent accounts being opened in their names." *In re Vtech Data Breach Litig.*, 2017 WL 2880102, at *4. There, the Court was unconvinced the plaintiffs' fear that dissemination of this information could compromise their other online accounts, such as PayPal, because they failed to

"provide a logical explanation as to how the disclosure of their Vtech login credentials would make fraudulent charges or identity theft likely" absent mere speculation. *Id.*; *see also Cooper*, 2022 WL 170622, at *3–4 (noting that claims of hackers using IP addresses are "entirely speculative, if not fanciful, and thus insufficient to support standing.").

Here, too, there is no logical explanation as to how disclosure of the information obtained in this breach, most of which is mundane and/or readily available online, increases their risk of identity theft without engaging in significant speculation. Plaintiffs' reliance on *Gaddy v. Long & Foster Companies, Inc.*, No. 21-2396, 2023 WL 1926654, at *8 (D.N.J. Feb. 10, 2023), does not alter this conclusion. There, the plaintiff alleged that her name, address, telephone number, Social Security number, W-2 details, and bank account information, among other non-public information, was potentially compromised in the data breach. *Gaddy*, 2023 WL 1926654, at *8. This is entirely different information than the information at issue in this breach. And even in *Gaddy*, the Court was skeptical that the plaintiffs' allegations of unauthorized credit card charges were directly traceable to the data breach but found that it was plausible enough at the motion to dismiss stage given the other information accessed since actors could "fill in the blanks of her financial accounts." *Id*. at *9. Here, it is not plausible, again, without engaging in speculation, that an actor could use the information obtained in this breach to make fraudulent charges or other identity theft.

In short, it is clear that the information obtained in this data breach is simply not sensitive enough to give rise to an imminent risk of identity theft or fraud for any Plaintiff. And this factor far outweighs the other factors.

Because there is no imminent risk of identity theft or fraud, Plaintiffs' other theories of injury—incurred costs associated with prophylactic measures, diminished value of PII, lost benefit

of the bargain, and emotional distress—alone cannot maintain a cause of action. *See In re Am. Fin. Res., Inc. Data Breach Litig.*, 2023 WL 3963804, at *5 ("All other injuries alleged by [the plaintiff] are inadequate because they rely on the unsupported assumption that his information will be imminently misused.").

Specifically, as to Plaintiffs' alleged time and money expenditures to monitor their accounts, the Third Circuit in *Reilly* held that "costs incurred to watch for a speculative chain of future events based on hypothetical future criminal acts are" not injuries which can confer standing. 664 F.3d at 46 (collecting cases). The Court explained, "that a plaintiff has willingly incurred costs to protect against an alleged increased risk of identity theft is not enough to demonstrate a 'concrete and particularized' or 'actual or imminent' injury. *Id.* (citing *Randolph v. ING Life Ins. & Annuity Co.,* 486 F. Supp. 2d 1, 8 (D.D.C. 2007)); *see also Allison v. Aetna, Inc.,* No. 09–2560, 2010 WL 3719243, at *5 n. 7 (E.D. Pa. Mar. 9, 2010) (rejecting claims for time and money spent on credit monitoring due to a perceived risk of harm as the basis for an injury in fact). Two years later, the Supreme Court held that a plaintiff "cannot manufacture standing by choosing to make expenditures based on hypothetical future harm that is not certainly impending." *Clapper*, 568 U.S. at 402. The Court reasoned, "[i]f the law were otherwise, an enterprising plaintiff would be able to secure a lower standard for Article III standing simply by making an expenditure based on a nonparanoid fear." *Id.* at 416. And, "[t]his rule from *Clapper* has been applied in the data breach context, such that courts have concluded that mitigation efforts following a data breach do[es] not confer standing where the alleged harm is not imminent." *Fero v. Excellus Health Plan, Inc.*, 236 F. Supp. 3d 735, 754 (W.D.N.Y. 2017) (collecting cases); *see also McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295, 304 n. 7 (2d Cir. 2021) (explaining costs associated with

prophylactic measures does not create an injury when the plaintiff cannot show a substantial risk of future identity theft).

Similarly, courts have held that emotional distress does not constitute an injury-in-fact in the absence of a substantial risk of future harm. *See In re Retreat Behav. Health LLC*, 2024 WL 1016368, at *3 ("While the additional harms outlined by Plaintiff, namely her emotional distress and time and money involved in mitigating the effects of the data breach, could be construed as *concrete* under *Clemens*, the injury still cannot be said to be *imminent* in the absence of any allegation that the information has been used in any manner.").

As for lost value of their PII and benefit of the bargain,"[c]ourts have rejected allegations that the diminution in value of personal information can support standing." *Fero*, 236 F. Supp. 3d at 755 (collecting cases); *see also Welborn v. Internal Revenue Serv.*, 218 F. Supp. 3d 64, 78 (D.D.C. 2016) ("Courts have routinely rejected the proposition that an individual's personal identifying information has an independent monetary value."); *Khan v. Children's Nat'l Health Sys.*, 188 F. Supp. 3d 524, 533 (D. Md. 2016) (rejecting diminution in value theory because plaintiff did not "explain how the hackers' possession of that information has diminished its value, nor does she assert that she would ever actually sell her own personal information"); *Whalen v. Michael Stores Inc.*, 153 F. Supp. 3d 577, 582 (E.D.N.Y. 2015), *aff'd*, *Whalen v. Michaels Stores, Inc.*, 689 F. App'x 89 (2d Cir. 2017) ("[W]ithout allegations about how her cancelled credit card information lost value, [plaintiff] does not have standing on this ground."); *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 30 (D.D.C. 2014) ("As to the value of their personal and medical information, Plaintiffs do not contend that they intended to sell this information on the cyber black market in the first place, so it is uncertain how they were

injured by this alleged loss. Even if the service members did intend to sell their own data—something no one alleges—it is unclear whether or how the data has been devalued by the breach.").

And even if any Plaintiff could show an imminent risk of identity theft, there is no causal link between any perceived risk of identity theft and this breach based on the nature of the information involved.

B. Traceability

Assuming Plaintiffs could show an imminent risk of identity theft—and they cannot—Article III standing further requires a "causal connection between the injury and the conduct complained of . . . ." *Lujan*, 504 U.S. at 560. In other words, the injury must be fairly traceable "to the challenged action of the defendant," though it need not be "certainly traceable." *Id.* Thus, proximate cause is not required to satisfy Article III's causation requirement. *Id*. In fact, "even harms that flow indirectly from the action in question can be said to be 'fairly traceable' to that action for standing purposes." *Focus on the Family v. Pinellas Suncoast Transit Auth.*, 344 F.3d 1263, 1273 (11th Cir. 2003). Yet, the traceability requirement cannot be satisfied when the party's theory of injury is based on a "speculative chain of possibilities." *Lujan*, 568 U.S. at 410.

Courts have rejected traceability arguments when the information needed to commit the alleged identity theft was not obtained in the data breach. *See I.C.*, 600 F. Supp. 3d at 1051 (noting "the SAC does not plausibly allege that any of I.C.'s information stolen in the data breach could be used to set up an account with a financial institution, such as a social security number[.]"); *Fernandez v. Leidos, Inc.*, 127 F. Supp. 3d 1078, 1086 (E.D. Cal. 2015) ("Plaintiff's allegations that someone attempted to open a bank account in his name, attempted to log in to his email

accounts, and that he received an increased number of email advertisements targeting his medical conditions do not allege injuries in fact fairly traceable to the Data Breach, since Plaintiff has not alleged that bank account information or email addresses were on the stolen backup data tapes."); *Antman*, 2015 WL 6123054, at *11 ("[Plaintiff] specifies disclosure only of his name and drivers' license information. It is not plausible that a person could apply for a credit card without a social security number[.]").

In *In re Science Applications International Corp. (SAIC) Backup Tape Data Theft Litigation*, the Court held that the plaintiffs' allegations of identity theft and fraud stemming from unauthorized credit card charges could not be causally linked to the breach because no plaintiff had alleged that credit card, debit card, or financial information was on the stolen tapes nor offered a plausible explanation for how a thief would have obtained this information in the data breach at issue. 45 F. Supp. 3d 14, 31 (D.D.C. 2014). "If certain 'information [is] not on the [stolen] tapes . . . Plaintiff[ ] cannot causally link [the use of that information] to the [Data Breach].'" *Fernandez*, 127 F. Supp. 3d at 1086 (alterations in original) (citing *SAIC*, 45 F. Supp. 3d at 31); *but see Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1327 (11th Cir. 2012) ("Plaintiffs allege that the same sensitive information that was stored on the stolen laptops was used to open the Bank of America account," and therefore, "Plaintiffs' allegations that the data breach caused their identities to be stolen move from the realm of the possible into the plausible."). In so concluding, the Court in *SAIC* noted the frequency of identity theft. *SAIC*, 45 F. Supp. 3d at 31 (citation omitted) ("In a society where around 3.3% of the population will experience some form of identity theft—regardless of the source—it is not surprising that at least five people out of a group of 4.7 million happen to have experienced some form of credit or bank-account fraud.").

Similarly, here, based upon the nature of the information involved in the data breach, there is no plausible explanation for how a thief obtained Plaintiffs' financial information without engaging in a series of hypotheticals, most of which would need to involve sophisticated social engineering to come to fruition. *See In re Horizon Healthcare Servs., Inc. Data Breach Litig.*, 2015 WL 1472483, at *8 (concluding that plaintiff's causation theory that his personal information was taken from defendant's laptop and combined with his wife's personal information from an unidentified source demonstrated the "remote possibility, rather than the plausibility, that the fraudulent tax return was connected to the Horizon laptop theft. Accordingly, [plaintiff's] tax fraud injury is not 'fairly traceable' to [d]efendant."). There is simply no plausible explanation for how Plaintiffs' alleged harm—like fraudulent charges—are linked in any way to the information, most of which is public information, involved in this data breach.

Overall, Plaintiffs fail to establish an injury that is certainly impending or fairly traceable to Defendant.[1] Thus, the Court finds that Plaintiffs lack Article III standing to pursue their claims. Having so found, the Court need not consider whether Plaintiffs' Complaint would pass muster under Rule 12(b)(6).

C. Fact Sheets

Though the Court did not consider the information contained in the Fact Sheets to reach its decision, the Court would reach the same result if it were to rely on the Fact Sheets. The chronology of this case presents circumstances where the parties have already exchanged some preliminary discovery. Indeed, such preliminary discovery was done at the behest of Plaintiffs and over the

[1] Because Plaintiffs fail to establish an injury-in-fact, and less so one that is linked to the Data Breach, the Court need not reach the issue of redressability.

Defendant's objections that no discovery should be permitted pending its then intended motions to dismiss. To be sure, the allegations in this case have greatly evolved since the inception of this case, and four iterations of the Complaint, based primarily upon the Facts Sheets exchanged by the parties. Significantly, the prior iterations of the Complaint alleged considerably more sensitive information was the subject of the data breach, such as social security numbers and financial account information, which were removed following the receipt of the Fact Sheets as Plaintiffs can no longer plausibly plead those allegations. And, as Defendant correctly notes, (Def. Br., ECF No. 185 at 14), it was the receipt of the Fact Sheets that prompted Plaintiffs' request to file the Third Amended Complaint, and later Fourth Amended Complaint, while the prior motions to dismiss were pending. *See* (ECF No. 117 at 11:6–14). Though the Court acknowledges the procedural posture in which this Motion is brought, it cannot ignore—nor can Plaintiffs evade—the information revealed in the fact sheets. Critically, Plaintiffs specifically reference, rely on, and *incorporate* the responses to the Fact Sheets into the Fourth Amended Complaint:

> Plaintiffs are unaware of the full extent of their PII in Samsung's [redacted] because Samsung has withheld complete information exfiltrated during the Data, while also downplaying the scope of the affected information. *Accordingly, the allegations about Plaintiffs' PII contained in the* [redacted] *are based on Samsung's Fact Sheet responses*.

(Am. Compl., ECF No. 147, ¶ 156) (emphasis added).

Though, at this stage, courts may not consider matters extraneous to the pleadings, "an exception to the general rule is that a document *integral to or explicitly relied* upon in the complaint may be considered without converting the motion [to dismiss] into one for summary judgment." *In re Burlington Coat Factory Sec. Litig.*, 114 F.3d 1410, 1426 (3d Cir. 1997) (emphasis added) (internal citations and quotation marks omitted); *see also In re Donald J. Trump Casino Sec. Litig.-*

Taj Mahal Litig., 7 F.3d 357, 368 n.9 (3d Cir. 1993) (citation omitted) ("[A] court may consider an undisputedly authentic document that a defendant attaches as an exhibit to a motion to dismiss if the plaintiff's claims are based on the document."). "The rationale underlying this exception is that the primary problem raised by looking to documents outside the complaint—lack of notice to the plaintiff—is dissipated '[w]here plaintiff has actual notice . . . and has relied upon these documents in framing the complaint.'" *Id*. (quoting *Watterson v. Page,* 987 F.2d 1, 3–4 (1st Cir. 1993)). The Court finds that to be the case here. There can be no doubt that Plaintiffs had actual notice of the Fact Sheets—having specifically requested leave to file the Third, and later Fourth, Amended Complaints, after the first iteration of this motion had been fully briefed, *based on the information contained in the Fact Sheets*—and has relied on the Facts Sheet, *see* (Am. Compl., ECF No. 147, ¶ 156), in framing the allegations of the Amended Complaint. Thus, the Court could have properly considered them.

And when the Court considers the information contained in the Fact Sheets, it reaches the same result: Plaintiffs fail to establish an injury that is certainly impending or fairly traceable to Defendant. Indeed, the Fact Sheets cast even more doubt as to Plaintiffs' allegations and speculation for several reasons.

First, some of the Plaintiffs indicated that some of the Samsung devices they purchased over the years were for family members. (Gilman Dec., ECF No. 162-21, Ex. B at B-276). That some Plaintiffs purchased devices for family members undoubtedly further weakens any claim that IMEI numbers obtained in the data breach subjects *them* to an increased risk of identity theft or fraud.

Second, for three of the four Plaintiffs who alleged that they have been notified that their information is on the Dark Web, the Fact Sheet unequivocally refutes any link to the breach. Plaintiff Baker, who alleged his information is on the Dark Web, stated in his Fact Sheet that Experian notified him that it found "records associated with [his Social Security Number] on the Dark Web." (Gilman Dec., ECF No. 162-21, Ex. B at B-495). As social security numbers were not obtained in this Data Breach, the fact that his data is on the Dark Web is wholly unrelated, and not plausibly traceable, to this breach. Plaintiff Peavy stated in her Fact Sheet that she was first notified that her information was on the Dark Web as early as 2018—four years before the Data Breach in 2022—and as such, this, too, cannot be linked to Defendant. (Gilman Dec., ECF No. 162-21, Ex. B at B-226–29). And finally, Plaintiff Allen stated that his email and other "information" was found on the Dark Web in June 2022—one month *before* the July 2022 Data Breach. (Gilman Dec., ECF No. 162-21, Ex. B at B-374, B-376-77).

Third, many of the Fact Sheet responses reinforce that the information obtained in this Data Breach could not have caused the injuries alleged. As Defendant notes, Plaintiff Curtis alleges a credit card was opened in his name following the data breach, (Am. Compl., ECF No. 147, ¶ 213), but the Fact Sheet states that only his name, email address, and IMEI number were disclosed in the breach. (Gilman Dec., ECF No. 162-20, Ex. A at A-011). Plaintiff Seirafi alleges his email account was hacked and his phone number was stolen in an attempt to hack his Crypto account, (Am. Compl., ECF No. 147, ¶ 177), but only his country and age group were disclosed according to the Fact Sheet. (Gilman Dec., ECF No. 162-20, Ex. A at A-010). And Plaintiffs Malota and Rollins assert attempted fraud, (Am. Compl., ECF No. 147, ¶¶ 233–38), despite the Fact Sheet indicating that none of their information was obtained in the Data Breach. (Gilman

Dec., ECF No. 162-20, Ex. A at A-012). In addition to these specific samples, the Fact Sheets also reveal that thirteen named Plaintiffs suffered identity theft *prior* to the 2022 data breach. (Gilman Dec., ECF No. 162-21, Ex. B at B-068, B-080, B-175, B-201, B-229, B-255–56, B-304, B-317, B-330, B-353, B-364, B-423, B-436).

In summary, though it would be proper to consider the Fact Sheets under the posture of this case, the Court did not do so and even if considered, the information contained in the Fact Sheets bolsters the conclusion that Plaintiffs plainly lack standing.

Finally, recognizing that the Complaint has been amended three times now, including twice after the receipt of the responses to the Fact Sheets, and because the Court cannot perceive what amendments could possibly cure the standing deficiencies described herein, the dismissal of these claims is with prejudice. Indeed, where a "plaintiff had already amended plaintiff's complaint and yet failed to allege sufficient facts, the courts may find that '[t]hree bites at the apple is enough,' and conclude that it is proper to deny leave to replead." *In re Intelligroup Sec. Litig.*, 527 F. Supp. 2d 262, 379 (D.N.J. 2007) (citing *Salinger v. Projectavision, Inc.*, 972 F. Supp. 222, 236 (S.D.N.Y. 1997)).

The Court, recognizes, as other courts have, the serious harm that identity theft and fraud poses but not every data breach results in an injury especially, here, when much of the information stolen is already public and/or not sensitive enough to give rise to identity theft. Given the fact that Plaintiffs have already amended the Complaint four times including after the benefit of Fact Sheets, a previous fully briefed motion to dismiss, and the Court having previously identified critical issues present in the case—most significantly, Plaintiffs' ability to link the data breach to their alleged harm—Defendant's Motion to Dismiss is granted and the dismissal is with prejudice.

See I.C., 600 F. Supp. 3d at 1055 ("Plaintiffs have already amended their pleadings after Zynga's prior motion to dismiss, and they fail to show how amendment could demonstrate a cognizable injury suffice to support Article III standing. Because Article III standing is an essential ingredient for subject matter jurisdiction in federal court . . . the case is dismissed with prejudice").

CONCLUSION

For the foregoing reasons, Defendant's Motion to Dismiss is **GRANTED**. (ECF No. 161). Plaintiffs' Fourth Amended Consolidated Complaint is dismissed with prejudice. For those matters initiated in state court, Docket Nos. 23-915, 23-917, 23-918, and 23-1019, they are remanded back to the respective state courts. As such, Defendant's Motion to Strike Class Allegations is **DENIED** as moot. (ECF. No. 163). An appropriate Order accompanies this Opinion.

CHRISTINE P. O'HEARN
United States District Judge